EXHIBIT 3

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, _____ a Special Agent (SA) with Homeland Security Investigations (HSI), being duly sworn, depose and state as follows:

INTRODUCTION

1. I have been employed as a Special Agent of the U.S. Department of Homeland Security, Homeland Security Investigations (HSI) since _____, and am currently assigned to _____. While employed by HSI, I have investigated federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography. I have gained experience through training at _____ and everyday work relating to conducting these types of investigations. I have received training in the area of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. **[DESCRIBE OTHER EXPERIENCE AND TRAINING IN CHILD PORNOGRAPHY INVESTIGATIONS]**. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2252 and 2252A, and I am authorized by law to request a search warrant.

2. **[PLEASE ONLY INSERT THE VIOLATIONS APPLICABLE TO YOUR TARGET]** This affidavit is submitted in support of an application for a search warrant for the locations specifically described in Attachment A of this Affidavit, including the entire property located at _____ (the "SUBJECT PREMISES") [and any person located at the SUBJECT PREMISES,] for contraband and evidence, fruits, and instrumentalities of violations of Title 18,

United States Code, Sections 2252 and 2252A, which items are more specifically described in Attachment B of this Affidavit.

3. The statements in this affidavit are based in part on information provided by HSI agents in Wilmington, Delaware, and Nogales, Arizona, and on my investigation of this matter. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of [**PLEASE ONLY INSERT THE VIOLATIONS APPLICABLE TO YOUR TARGET**] 18 U.S.C. §§ 2252(a)(1) and (b)(1) (transportation of a visual depiction of a minor engaged in sexually explicit conduct); 18 U.S.C. §§ 2252(a)(2) and (b)(1) (distribution of a visual depiction of a minor engaged in sexually explicit conduct); 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) (possession of and access with intent to view a visual depiction of a minor engaged in sexually explicit conduct); 18 U.S.C. §§ 2252A(a)(1) and (b)(1) (transportation of child pornography); 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1) (distribution of child pornography); and 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) (possession of and access with intent to view child pornography), are presently located at the SUBJECT PREMISES.

STATUTORY AUTHORITY

4. [**PLEASE ONLY INSERT THE VIOLATIONS APPLICABLE TO YOUR TARGET**] As noted above, this investigation concerns alleged violations of the following:

a. Title 18, United States Code, Sections 2252(a)(1) and (b)(1) prohibit any person from knowingly transporting or shipping, or attempting or conspiring to transport

or ship, any visual depiction using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce, by any means including by computer or mails, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

b. Title 18, United States Code, Sections 2252(a)(2) and (b)(1) prohibit any person from knowingly receiving or distributing, or attempting or conspiring to receive or distribute, any visual depiction using any means or facility of interstate or foreign commerce, or that has been mailed or shipped or transported in or affecting interstate or foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means including by computer, or knowingly reproducing any visual depiction for distribution using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce or through the mails, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

c. Title 18, United States Code, Sections 2252(a)(4)(B) and (b)(2) prohibit any person from knowingly possessing or accessing with the intent to view, or attempting or conspiring to possess or access with the intent to view, 1 or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer, if the production of such visual depiction involved the use

of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

d. Title 18, United States Code, Sections 2252A(a)(1) and (b)(1) prohibit a person from knowingly mailing, or transporting or shipping using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, any child pornography, as defined in 18 U.S.C. § 2256(8), or attempting or conspiring to do so.

e. Title 18, United States Code, Sections 2252A(a)(2)(A) and (b)(1) prohibit a person from knowingly receiving or distributing, or attempting or conspiring to receive or distribute, any child pornography or any material that contains child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

f. Title 18, United States Code, Sections 2252A(a)(5)(B) and (b)(2) prohibit a person from knowingly possessing or knowingly accessing with intent to view, or attempting or conspiring to do so, any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

DEFINITIONS

5. The following definitions apply to this Affidavit and Attachment B:

a. "Chat," as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

b. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors in sexually explicit poses or positions.

c. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

d. "Cloud-based storage service," as used herein, refers to a publicly accessible, online storage provider that collectors of child pornography can use to store and trade child pornography in larger volumes. Users of such a service can share links and associated passwords to their stored files with other traders of child pornography in order to grant access to their collections. Such services allow individuals to easily access these files through a wide variety of electronic devices such as desktop and laptop

computers, mobile phones, and tablets, anywhere and at any time. An individual with the password to a file stored on a cloud-based service does not need to be a user of the service to access the file. Access is free and readily available to anyone who has an Internet connection.

e. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, and mobile phones and devices. *See* 18 U.S.C. § 1030(e)(1).

f. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

g. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually

operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

h. "File Transfer Protocol" ("FTP"), as used herein, is a standard network protocol used to transfer computer files from one host to another over a computer network, such as the Internet. FTP is built on client-server architecture and uses separate control and data connections between the client and the server.

i. "Hashtag," as used herein, refers to a word or phrase preceded by a hash or pound sign (#), which is used to identify messages or groups on a specific topic.

j. "Internet Protocol address" or "IP address," as used herein, refers to a unique number used by a computer or other digital device to access the Internet. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet.

k. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the

conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

BACKGROUND ON CHILD PORNOGRAPHY, COMPUTERS, THE INTERNET, AND EMAIL

6. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers and digital technology have dramatically changed the way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Child pornographers can now transfer printed photographs into a computer-readable format with a device known as a scanner. Furthermore, with the advent of digital cameras and smartphones with cameras, when the photograph is taken it is saved as a digital file that can be directly transferred to a computer by simply connecting the camera or smartphone to the computer. In the last ten years, the resolution of pictures taken by digital cameras and smartphones has increased dramatically, meaning that such pictures have become sharper and crisper. Photos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards often store up to 32 gigabytes of data, which provides enough space to store thousands of high-resolution photographs. Video camcorders, which once recorded video onto tapes or mini-CDs, now can save video

footage in a digital format directly to a hard drive in the camera. The video files can be easily transferred from the camcorder to a computer.

c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTPs) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (*i.e.*, "instant messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. In addition, there are numerous options available for the storage of computer or digital files. One-terabyte external and internal hard drives are not uncommon. Other media storage devices include CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices which are plugged into a port on the computer. It is extremely easy for an individual to take a photo or a video with a digital

camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices (CDs and DVDs are unique in that special software must be used to save or "burn" files onto them). Media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer or external media in most cases.

g. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (*i.e.*, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files). Digital information can also be retained unintentionally such as the traces of the path of an electronic communication may be automatically stored in many places (*e.g.*,

temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

7. Based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to "cloud" storage. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software application, or operating system that is being searched;

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted;

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened.

Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

8. Based on my own experience and my consultation with other agents who have been involved in computer searches, searching computerized information for contraband, evidence, fruits, or instrumentalities of a crime often requires the seizure of all of a computer system's input and output peripheral devices, related software, documentation, and data security devices (including passwords), so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment. There are several reasons that compel this conclusion:

a. The peripheral devices that allow users to enter or retrieve data from the storage devices vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output devices in order to read the data on the system. It is important that the analyst be able to properly re-configure the system as it now operates in order to accurately retrieve the evidence listed above. In addition, the analyst needs the relevant system software (operating systems, interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instruction manuals or other documentation and data security devices; and

b. In order to fully retrieve data from a computer system, the analyst also needs all magnetic storage devices, as well as the central processing unit (CPU). Further, the analyst needs all the system software (operating systems or interfaces, and hardware

drivers) and any applications software that may have been used to create the data (whether stored on hard drives or on external media) for proper data retrieval.

9. Additionally, based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of so-called "wireless routers," which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be "secured" (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or "unsecured" (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

PROBABLE CAUSE

10. In February of 2014, HSI agents in Wilmington, Delaware, and Nogales, Arizona, began investigating an online mobile chat application used extensively by persons interested in

exchanging child pornography and/or sexually abusing children. This chat application is hereinafter referred to as "Application A."[1]

11. "Application A" is designed for mobile chatting or messaging. To use this application, a user downloads the application to a mobile phone or other mobile device via a service such as Google Play Store, Apple iTunes, or another similar provider. Once downloaded and installed, the user is prompted to create an account and username. The user also has a display name, which is what other users see when transmitting messages back and forth. Once the user has created an account, the user is able to locate other users via a search feature, and the two parties can then send messages, images, and videos between them.

12. "Application A" users are also able to create chat groups, of up to 50 people, to communicate in a group setting and exchange images and videos. These groups are administered by the creator who has the authority to ban and remove other users from the created group. Once the group is created, "Application A" users have the option of sharing a link to the group with all of their contacts or any other user. These groups are frequently created with a "hashtag" that is easily identifiable or searchable by keyword.

13. Within the child pornography trading communities on "Application A," actual chat group names have included "#TradeChildPorn," "#Kindergarten," "#Pedosplayhouse," "#TradeYoungGirlPics," "#Kidsxxx," "#Young," "#Pedisex," and "#Drilledkid." "Application

[1] The actual name of "Application A" is known to law enforcement. This chat application remains active and disclosure of the name of the application would potentially alert its users to the fact that law enforcement action is being taken against users of the application, thereby provoking users to notify other users of law enforcement action, flee, and/or destroy evidence. Accordingly, to protect the confidentiality and integrity of the ongoing investigation involved in this matter, specific names and other identifying factors have been replaced with generic terms and the application will be identified herein as "Application A."

A" users within these chat groups are frequently banned or removed for their failure to post child pornography within a specific period of time determined by the administrator. The chat groups also are a means to meet like-minded users who can then chat and trade child pornography through the direct chat feature. "Application A" users can also provide to each other links and/or password access to larger quantities of child pornography that are stored in a cloud-based storage service.

14. **[INCLUDE ANY OF THE FOLLOWING THAT YOU DEEM RELEVANT]** On _____, an HSI agent located in _____, acting in an undercover capacity and using a device connected to the Internet, signed into an "Application A" user account and entered "Application A" chat group "_____." At approximately _____, this agent observed that "Application A" user _____ with the display name _____ ("SUBJECT ACCOUNT") had posted at least __ image(s) and __ video(s) of child pornography, *i.e.,* visual depictions of a minor engaging in sexually explicit conduct, in this chat group on _____, at approximately _____. The undercover agent was able to download and save these image(s) and video(s) to an undercover device. These image(s) and video(s) included the following:

a. "**[INSERT FILE NAME]**," which depicts _____.

b. "**[INSERT FILE NAME]**," which depicts _____.

c. "**[INSERT FILE NAME]**," which depicts _____.

[INSERT ANY ADDITIONAL PROBABLE CAUSE FOR VIOLATIONS FOUND REGARDING THE SUBJECT ACCOUNT, INCLUDING ANY RELEVANT CHAT GROUP COMMUNICATIONS BETWEEN THE SUBJECT ACCOUNT USER AND OTHER "APPLICATION A" USERS, AND/OR DIRECT COMMUNICATIONS BETWEEN THE SUBJECT ACCOUNT USER AND AN HSI UNDERCOVER AGENT]

15. On _____, a U.S. Immigration and Customs Enforcement summons was served on "Application A" for subscriber and login information related to the SUBJECT ACCOUNT. A review of the results obtained on _____ revealed the following information regarding the subscriber: _____. The results also revealed that a user of the SUBJECT ACCOUNT logged in from the following IP address(es) on the dates and times specified: [**INSERT IP ADDRESS(ES) AND DATES/TIMES**].

16. A query of the American Registry for Internet Numbers ("ARIN") online database revealed that IP address _____ was registered to **[INSERT ISP].**

17. On _____, a U.S. Immigration and Customs Enforcement summons was issued to **[INSERT ISP]** in regard to the IP address(es) described in Paragraph __. A review of the results obtained on _____ identified the following account holder and address, which is the address of the SUBJECT PREMISES: _____.

[ADD ONE OR MORE OF THE FOLLOWING CONFIRMING TARGET'S RESIDENCE AND ANY OTHER TYPE OF RECORD CHECKS NOT LISTED]

18. A check of publicly available databases also revealed that _____ resides at the SUBJECT PREMISES.

19. A check with the Division of Motor Vehicles on or about [**insert date**] revealed that an individual named [**target's name**] with a date of birth of [**insert date**] resides at the SUBJECT PREMISES.

20. On or about **[insert date]** representatives of the U.S. Postal Service stated that **[subject's name]** is currently receiving mail at the SUBJECT PREMISES.

21. On or about [**insert date**] representatives of **[local utilities company]** indicated that service is being provided to **[insert target's name]** at the SUBJECT PREMISES.

22. Surveillance of the SUBJECT PREMISES on or about **[insert date]** revealed that **[insert facts]**.

23. **[To the extent required or expected in your district, include language regarding whether an open, unsecure wireless access point exists at or near the SUBJECT PREMISES. Note that generally, law enforcement is not required to determine whether one exists because an open, unsecure wireless access point does not undermine probable cause that the SUBJECT PREMISES will contain evidence of the offense.** ***See United States v. Perez*****, 484 F.3d 735, 740 (5th Cir. 2007);** ***United States v. Thomas*****, 2012 WL 4892850, at *3-4 (D. Vt. 2012);** ***United States v. Larson*****, 2011 WL 3837540, at *2-6 (W.D. Mo. 2011);** ***United States v. Courtney*****, 2008 WL 4998997, at *4 (E.D. Ark. 2008);** ***United States v. Carter*****, 549 F. Supp. 2d 1257, 1268-69 (D. Nev. 2008). However, if law enforcement is aware that an open, unsecure wireless access point exists at or near the SUBJECT PREMISES, it would be prudent to include such information in the search warrant affidavit to avoid any possible** ***Franks*** **issues.]** On or about [**insert date**], I used a [**insert name of wireless-sniffer device**] wireless device in an effort to gain additional information regarding any potential wireless networks at the SUBJECT PREMISES. Positioned [**state location relative to**] the SUBJECT PREMISES, I noted that [**SELECT ONE:**] [there were multiple wireless networks in the area, but all of them were secured. Accordingly, in order to use any of them to access the Internet, a user would likely have to know the encryption key or password for that particular network.] [**OR**] [there were both secured and unsecured wireless networks in the area]. Based

on [**INCLUDE ALL APPLICABLE REASONS**] [the signal strength of the wireless networks] [the names, or Service Set Identifiers, of the wireless networks][(other relevant information)], as well as my training and experience and information related to me by agents, I believe that the wireless router at the SUBJECT PREMISES is likely generating a [**SELECT ONE:**] [secured] [unsecured] wireless network.] [**OR**] [there were multiple wireless networks in the area, and all of them were unsecured.] As explained above, I know, from my training and experience and information related to me by agents that wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime.

24. A search of Accurint information database (a public records database that provides names, dates of birth, addresses, associates, telephone numbers, email addresses, etc.) was conducted for **[target]**. These public records indicated that **[target's]** current address is **[address]**.

25. A check of open source information from the Internet regarding [**target**] revealed [**insert any relevant info related to target, his past, access to children, etc.**]

PAST CHILD EXPLOITATION CONDUCT/ACTIVITY OF [TARGET]

[Research the suspect's federal and state records and check with state and federal agencies to determine whether the suspect has prior criminal violations involving child sexual abuse, child pornography, and other sexual exploitation crimes, or has been a suspect in another similar federal or state investigation. Background investigation sources should include information maintained by the National Center for Missing and Exploited Children (NCMEC). In *United States v. Lapsins*, 570 F.3d 758 (6th Cir. 2009), the court held that information that was more than one year old was not stale because the affidavit was also supported by information from

NCMEC that the defendant had downloaded more than 100 images one month before the warrant was executed. *See id.* at 767 ("[NCMEC] information was reliable enough to contribute to a finding of probable cause, it remedied any potential staleness defect."). State database checks should include the suspect's current state of residency as well as all other states in which the suspect has resided. If the state and federal checks reveal relevant prior offenses or involvement in other, similar investigations, this information should be included in the affidavit for the purpose of establishing a pattern of similar criminal activity that supports probable cause for the instant search warrant. In *United States v. Perrine*, 518 F.3d 1196, 1205 (10th Cir. 2008), the court rejected the defendant's challenge to the search warrant, in part, because it contained additional information regarding the defendant's previous state conviction in Kansas for exploitation of a child, his current probation for that offense, and because the prior offense involved the same activity under federal investigation.]

CHARACTERISTICS COMMON TO INDIVIDUALS WHO TRANSPORT, DISTRIBUTE, POSSESS, AND/OR ACCESS WITH INTENT TO VIEW CHILD PORNOGRAPHY

[revise title to match the facts of your specific target]

[NOTE: Use this language ONLY if the target fits the profile and you are comfortable with stating it based on your experience with these cases. CRITICAL: you must tie these characteristics to the specific offender. Because this operation encompasses a wide range of conduct please go through and modify language for your particular offender.]

26. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who [transport, distribute, possess, and/or access with intent to view child pornography (**add any additional violation specific to your Target**)]:

a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Such individuals almost always possess and maintain their hard copies of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the

possessor's vehicle, or, at times, on their person, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis; however, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools.

e. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. Such individuals prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world. Thus, even if [target name] uses a portable device (such as a mobile phone) to access the internet and child pornography, it is more likely than not that evidence of this access will be found in his home, the SUBJECT PREMISES, [as well as (list other all locations that have been named in Attachment A),] as set forth in Attachment A.

27. Based on the following, I believe that the user of the SUBJECT ACCOUNT residing at SUBJECT PREMISES likely displays characteristics common to individuals who [transport, distribute, possess or access with intent to view child pornography]. For example, the

target of investigation:

[INSERT FACTS RELEVANT TO YOUR TARGET, INCLUDING CHAT GROUP COMMUNICATIONS BETWEEN THE SUBJECT ACCOUNT USER AND OTHER "APPLICATION A" USERS, AND/OR DIRECT COMMUNICATIONS BETWEEN THE SUBJECT ACCOUNT USER AND AN HSI UNDERCOVER AGENT; THE NAMES OF THE CHAT GROUPS OF WHICH THE TARGET WAS A MEMBER; THE NUMBER OF CHILD PORNOGRAPHY IMAGES AND VIDEOS THAT THE TARGET POSTED; THE PERIOD OF TIME OVER WHICH THE TARGET ENGAGED IN THESE ACTIVITIES (DAYS, WEEKS, MONTHS); AND RELEVANT PAST CHILD EXPLOITATION ACTIVITY/CONDUCT/HISTORY, ETC.]

REQUEST FOR SEALING OF APPLICATION/AFFIDAVIT

28. [SEALING LANGUAGE: Depending on your district, it may be necessary to make a separate motion to seal the warrant. If possible, the affidavit should be sealed not only until the warrant is executed, but until the operation is concluded.] It is respectfully requested that this Court issue an order sealing, until further order of this Court, all papers submitted in support of this Application, including the Application, Affidavit, and Search Warrant, and the requisite inventory notice (with the exception of one copy of the warrant and the inventory notice that will be left at the SUBJECT PREMISES). Sealing is necessary because the items and information to be seized are relevant to an ongoing investigation and not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that online criminals actively search for criminal affidavits and search warrants via the Internet, and disseminate them to other online criminals as they deem appropriate, *i.e.*, post them publicly online through forums. Premature disclosure of the contents of this Affidavit and

related documents may have a significant and negative impact on this continuing investigation and may jeopardize its effectiveness by alerting potential targets to the existence and nature of the investigation, thereby giving them an opportunity to flee, or to destroy or tamper with evidence.

CONCLUSION

29. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B, are located at the locations described in Attachment A. I respectfully request that this Court issue a search warrant for the locations described in Attachment A, authorizing the seizure and search of the items described in Attachment B.

30. I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, the "return" inventory will contain a list of only the tangible items recovered from the premises. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.

_____
AGENT'S NAME
Special Agent
Homeland Security Investigations

Sworn and subscribed before me this ___th day of ____, 2015.

_____
JUDGE'S NAME
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

DESCRIPTION OF LOCATIONS TO BE SEARCHED

The entire property located at [ADDRESS], including the residential building, any outbuildings, and any appurtenances thereto (the SUBJECT PREMISES). **[INSERT FURTHER DESCRIPTION OF THE SUBJECT PREMISES AND/OR A PICTURE OF THE SUBJECT PREMISES]**

[Any person located at the SUBJECT PREMISES.]

[As appropriate, include language justifying search of motor vehicles and edit relevant paragraphs of affidavit to include search of motor vehicle].

[If sufficient evidence and probable cause exists to identify one or more known individuals as the likely perpetrator(s) of the offense, consider adding the following language and editing relevant paragraphs of affidavit: The person of XXX (DOB: XX/XX/XXXX), provided that this person is located at the SUBJECT PREMISES and/or within the District of [insert district] at the time of the search.]

ATTACHMENT B

ITEMS TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, Sections 2252 and 2252A:

1. Computers or storage media used as a means to commit the violations described above.
2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
    a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
    b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
    c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crime(s) under investigation and to the computer user;

e. evidence indicating the computer user's knowledge and/or intent as it relates to the crime(s) under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

m. contextual information necessary to understand the evidence described in this attachment.

3. Routers, modems, and network equipment used to connect computers to the Internet.
4. Child pornography and child erotica.
5. Records, information, and items relating to violations of the statutes described above including:
    a. Records, information, and items relating to the occupancy or ownership of the SUBJECT PREMISES, [ADDRESS], including utility and telephone bills, mail envelopes, or addressed correspondence;
    b. Records, information, and items relating to the ownership or use of computer equipment found in the above residence, including sales receipts, bills for Internet access, and handwritten notes;
    c. Records and information relating to the identity or location of the persons suspected of violating the statutes described above;
    d. Records and information relating to the sexual exploitation of children, including correspondence and communications between users of "Application A";
    e. Records and information showing access to and/or use of "Application A"; and
    f. Records and information relating or pertaining to the identity of the person or persons using or associated with the [insert username/screen name].

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.